UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	Honorable James B. Clark, III
	:	
ISRAFIL "DAVID" DEMIR	:	Mag. No. 21-12219
	:	
	:	**FILED UNDER SEAL**

I, Robert S. Pinches, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations, and that this complaint is based on the following facts:

SEE ATTACHMENT B

Robert S. Pinches, Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations
Special Agent Robert S. Pinches attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to ~~before me and subscribed~~ via telephone on in my presence,
May 25, 2021, Essex County, New Jersey

Honorable James B. Clark, III
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Conspiracy to Commit Mail and Wire Fraud)

From at least as early as in or about September 2017 through the present, in Passaic County, in the District of New Jersey, and elsewhere, the defendant,

ISRAFIL "DAVID" DEMIR,

did knowingly and intentionally conspire and agree with others to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud, to cause to be delivered by mail according to the directions thereon matters and things to be sent and delivered by a private and commercial interstate carrier, and to transmit and cause to be transmitted by means of wire, radio, and television communications in interstate and foreign commerce certain writings, signs, signals, and sounds, contrary to Title 18, United States Code, Sections 1341 and 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Robert S. Pinches, am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background

1. At times relevant to this Complaint:

a. Business-1 was a New Jersey limited liability company incorporated in 2014. Business-1 maintained a warehouse in Woodland Park, New Jersey, which served as Business-1's primary place of business (the "Business-1 Warehouse").

b. The defendant, Israfil "David" Demir ("DEMIR"), resided in Secaucus, New Jersey. DEMIR was a principal of Business-1, and his email signatures for his Business-1 email account variously listed his title as either "Product Manager" or "Sales Manager." DEMIR's legal name was Israfil, but he also used the name "David," including in correspondence relating to Business-1.

c. Cisco Systems, Inc. ("Cisco") was a major U.S. technology conglomerate headquartered in San Jose, California. Among other services and products, Cisco designed, manufactured, and sold networking devices, *i.e.*, computer hardware that allowed computers connected by a network to communicate with each other. The networking devices relevant to this Complaint included "switches" and "transceivers," which are devices used to facilitate the transmission of signals between computers on a computer network.

d. I know from training, experience, and investigation that Cisco's networking devices are used in information networks in the United States and across the world. Many of these devices are purchased and used by U.S. government and military entities, hospitals, schools, and other critical sectors, and are used in sensitive and essential applications. A wide variety of critical infrastructure relies on such networking equipment to maintain the security and integrity of government, medical, and business data storage, transfer, and communications. Sensitive and important functions performed by the government, as well as both public-

and private-sector entities, rely on the performance of high-quality networking products. These functions are endangered by lower quality counterfeits.

e. I also know, from training, experience, and investigation, that counterfeit products that bear Cisco marks without permission provide customers with the false assurance that those products are reliable and conform with Cisco's standards, come with applicable Cisco warranties, can be immediately placed under a Cisco service support contract, and have been produced in accordance with Cisco's quality assurance standards.

f. I also know, from training, experience, and investigation, that counterfeit Cisco products often use pirated versions of Cisco software—in many cases, older and outdated software that does not necessarily operate correctly—leaving users exposed to security vulnerabilities that Cisco had detected and fixed in current and genuine software versions. For this reason, using counterfeit Cisco products can expose a user's network to security or intrusion vulnerabilities.

g. Supplier-1 was a supplier of counterfeit Cisco devices headquartered in Beijing, China. Supplier-1 was not affiliated with Cisco in any way and was not an authorized reseller or distributor of Cisco products.

h. CC-1 was a sales representative for Supplier-1.

Overview of the Conspiracy

2. An investigation conducted by HSI and the U.S. Department of Defense, Office of Inspector General ("DOD-OIG") has shown that DEMIR and others (the "Conspirators") have, from at least as early as September 2017 to the present, executed a scheme to knowingly import counterfeit Cisco networking devices from various illicit overseas suppliers, including suppliers based in China and Hong Kong (such as Supplier-1), and to then sell those counterfeit Cisco devices to U.S. customers as genuine Cisco products (the "Conspiracy").

3. During this time, DEMIR and the other Conspirators used various business entities owned or controlled by DEMIR and others, including Business-1 (the "Trafficking Business Entities"), to sell products that were packaged and built to resemble genuine Cisco networking devices. But in fact, at least a substantial portion—and, potentially, virtually all—of the Cisco products sold by DEMIR and the Conspirators through the Trafficking Business Entities were counterfeits (the "Counterfeit Cisco Products").

4. The numerosity of the Trafficking Business Entities appears to serve no legitimate business purpose. To the contrary, I know from training and

experience that counterfeit traffickers frequently form and conduct transactions through multiple business entities to evade detection, identification, and enforcement by either intellectual-property owners (like Cisco), marketplaces (like Amazon), and law enforcement.

5. Materials obtained by law enforcement, including bank records, records of deliveries by interstate carriers, and emails sent and received by the Conspirators from Business-1 email accounts, show that the Conspirators have acquired Counterfeit Cisco Products from multiple overseas suppliers. Some of these suppliers, such as Supplier-1, are situated in China and Hong Kong. I know from training, experience, and investigation that many suppliers and manufacturers of counterfeit Cisco products operate in China and Hong Kong, at least in part because of comparatively lax enforcement of U.S. intellectual property rights in those jurisdictions.

6. The Conspirators have sold the Counterfeit Cisco Products through multiple channels, including online marketplaces like Amazon, where the Conspirators have operated multiple online storefronts associated with the Trafficking Business Entities. The Conspirators also have sold Counterfeit Cisco Products directly from their own websites, also associated with various Trafficking Business Entities, many of which falsely touted the authenticity of the Cisco products for sale. For example, one such website purported that "[a]ll of [its] products are factory new sealed and clean serial."

Seized Shipments and Notifications to the Conspirators

7. Between September 2017 and the present, U.S. Customs officials have seized more than 20 shipments of purported Cisco networking devices, including switches and transceivers, from various suppliers in China, Hong Kong, and other overseas locations that were destined for various locations controlled by the Conspirators. The majority of these seized shipments were addressed to the Business-1 Warehouse. At least two of these seized shipments listed Supplier-1 as the named exporter. Many of the shipments listed bogus names for the importer, which I know, based on training and experience, to be a tactic used by counterfeit traffickers to evade detection.

8. Cisco has analyzed the supposed Cisco networking devices contained in these seized shipments. These products bore registered Cisco trademarks and were clearly designed and intended to mimic actual Cisco networking devices. Cisco has verified to law enforcement, however, that the supposed Cisco networking devices in the seized shipments were actually Counterfeit Cisco Products based on, among other indications, packaging irregularities and internal circuitry within these products.

9. The total manufacturer's suggested retail price ("MSRP") of the genuine analogues of the seized Counterfeit Cisco Products totals at least approximately $3.8 million.

10. It is standard procedure for U.S. Customs, after an international shipment is seized, to send a seizure notice to the listed importer on that shipment that articulates the basis for the seizure. In this matter, law enforcement has verified that such seizure notices were sent by U.S. Customs to the listed importer on each of the seized shipments of Counterfeit Cisco Products, and that these seizure notices advised that the shipments contained Counterfeit Cisco Products. The identifying information listed for the importer on these seized shipments included, in each instance, either (i) a Conspirator name, (ii) a Trafficking Business Entity name, and/or (iii) physical addresses known to be controlled by the Conspirators, such as the Business-1 Warehouse.

11. In addition, Cisco sent multiple cease-and-desist letters to the Conspirators and to the Trafficking Business Entities advising that the products included in the seized shipments were counterfeits and directing the Conspirators and Trafficking Business Entities to cease selling counterfeit Cisco products.

12. Notwithstanding these U.S. Customs seizure notices and Cisco cease-and-desist letters, the Conspirators have continued to import Counterfeit Cisco Products—frequently from many of the same suppliers that shipped the Counterfeit Cisco Products seized by U.S. Customs as described above.

Controlled Purchase

13. In August 2020, law enforcement visited the Amazon online storefront of a particular Trafficking Business Entity ("TBE-1") (the "TBE-1 Storefront"). Investigation has shown TBE-1 to be controlled by the Conspirators, and by DEMIR in particular. Records obtained from Amazon, for example, show that DEMIR's name was listed on the Amazon account of TBE-1, and the listed address on the TBE-1 account was the Business-1 Warehouse.

14. At that time, the TBE-1 Storefront advertised a particular model of a Cisco switch in "new" condition. The listed price was $1,455.52. By contrast, the MSRP of a genuine, new model of that switch is, according to Cisco, $12,793.30.

15. Law enforcement ordered the switch from the TBE-1 Storefront. The ordered switch was delivered in or around September 2020 (the "Controlled Counterfeit Switch"). The return address on the switch was "SHIPPING DEPARTMENT" at the Business-1 Warehouse address.

16. Cisco analyzed photographs of the switch provided by law enforcement and determined that the switch was a Counterfeit Cisco Product,

based on, among other indicators, serial numbers and other unique product-identifying numbers on the product that did not match entries in Cisco's manufacturing databases.

DEMIR's Knowledge of the Conspiracy

17. Evidence obtained during this investigation shows that DEMIR knew fully that the Cisco products that he and the other Conspirators were importing and selling were counterfeits.

18. ***The Demir Email Account.*** Law enforcement obtained by lawful search warrant and reviewed the contents of a Google-hosted email account used by DEMIR to conduct Business-1 business (the "Demir Email Account"). The email address of the Demir Email Account was "david@[Business-1][.]com." According to Google records, the Demir Email Account listed (a) DEMIR as the subscriber, and (b) a personal Gmail account in DEMIR's name as the recovery account. I believe, based on these facts, my review of email content, and my investigation, that the Demir Email Account is under DEMIR's personal control.

19. Emails from the Demir Email Account show that DEMIR conducted much of Business-1's procurement of Counterfeit Cisco Products from overseas suppliers. Supplier-1 was one prominent supplier of Counterfeit Cisco Products to the Conspirators, and CC-1 was DEMIR's regular contact there. DEMIR would frequently email CC-1 to inquire about inventory and pricing and to place orders.

20. In one such email exchange in December 2019:

a. A Business-1 customer had ordered and took shipment of Cisco networking devices from Business-1 in Fall 2019 (the "Fall 2019 Devices") and found during testing that those devices were Counterfeit Cisco Products. Specifically, Cisco devices contained codes, called "organizationally unique identifier" ("OUI") codes, that relate to where a given product was manufactured. In an email to the Demir Email Account, the customer explained that the Fall 2019 Devices contained OUI codes that pointed to a manufacturing location where genuine versions of those devices were never actually manufactured. I know from training, experience, and investigation that this type of mismatch in the OUI codes of Cisco devices is an indicator of counterfeiting. The customer also told DEMIR that it would quarantine the Fall 2019 Devices to avoid liability for trafficking in counterfeit products.

b. In response, DEMIR emailed the customer claiming that the Fall 2019 Devices had been procured from an authorized Cisco channel. As support, DEMIR attached partially redacted invoices for the Fall 2019 Devices bearing Cisco logos and trademarks, which I believe were intended to make these documents appear like authentic invoices of either Cisco itself or an authorized Cisco reseller.

c. In fact, however, emails in the Demir Email Account show that DEMIR had procured the Fall 2019 Devices from Supplier-1, not from either Cisco or an authorized Cisco reseller. I believe, therefore, that the invoices DEMIR sent to the customer were fabricated.

d. In this instance, ***after*** being alerted by the customer of the counterfeit issue, DEMIR emailed CC-1 not to ask whether Fall 2019 Devices were in fact genuine—but rather to ask CC-1 for "replacement parts" for the Fall 2019 Devices.

e. Later in or around December 2019, DEMIR emailed CC-1 again. DEMIR wrote:

> One of the engineer said [manufacturing location] [Cisco] modules never use [different manufacturing location] OUI ***and china still don't know that***. If they find out following instruction they will increase their ability ***and nobody can understand they are fake or not.*** 😊
>
> These are the issue. Copy that to your customer. They will understand.

(Emphasis added.) Beneath this text, DEMIR then provided the list of OUI codes that he had received from the customer indicating that the Fall 2019 Devices were Counterfeit Cisco Products.

21. In other words, DEMIR sought in this email to provide CC-1 with information that would enable Supplier-1 and its own supply chain to manufacture counterfeit Cisco products with proper OUI codes, making them more difficult to detect as counterfeits.

22. Emails in the Demir Email Account show that DEMIR and the Conspirators continued to procure and sell Cisco products from Supplier-1 even after receiving repeated indications that products shipped by Supplier-1 were Counterfeit Cisco Products. The Controlled Counterfeit Switch obtained by law enforcement in 2020—months after the correspondence regarding the Fall 2019 Devices—is one such product. Specifically, Emails in the Demir Email Account between DEMIR and CC-1 show that Business-1 had procured from Supplier-1 a Cisco device bearing the same serial number as the Controlled Counterfeit Switch in summer 2020—months after the December 2019 exchange described above. I believe, therefore, that DEMIR procured the Controlled Counterfeit Switch from Supplier-1 months ***after*** being placed on clear notice that Supplier-1 was a counterfeit trafficker (and, indeed, conspiring with Supplier-1 to manufacture counterfeit Cisco products that would be harder to detect).

23. ***Bank Records.*** Law enforcement has also obtained and reviewed records for a bank account under the name of one of the Trafficking Business

Entities, for which DEMIR is the sole signatory. Those records show that DEMIR has wired significant amounts of money to multiple overseas suppliers of Counterfeit Cisco Products during the Conspiracy. All told, DEMIR has wired over $1.2 million to bank accounts in China and Hong Kong, which law enforcement believes to be owned or controlled by the counterfeit suppliers used by the Conspirators. DEMIR has wired over $178,000 to Supplier-1 alone.